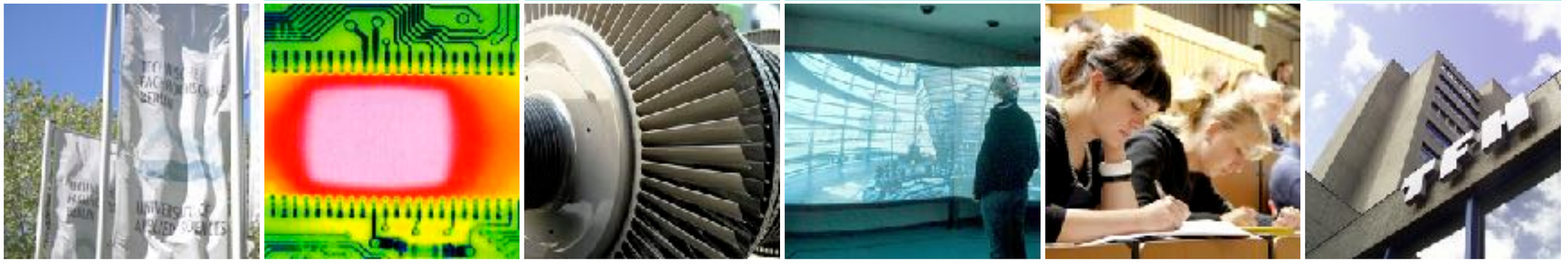
BEUTH HOCHSCHULE FÜR TECHNIK BERLIN
University of Applied Sciences

Offene Gebäudeautomation

Summer School

Kommunikationsprotokolle

EMR



Beuth Hochschule für Technik Berlin

Kommunikationsprotokolle

Die Hauptaufgabe jedes LANs besteht im Datenaustausch zwischen Anwendungsprogrammen (Applikationen), die sich auf unterschiedlichen Stationen befinden. Dafür sind bestimmte Regeln notwendig, die vor allem die Datenformate und die zeitliche Reihenfolge beim Datenaustausch festlegen. Diese Regeln werden als Kommunikationsprotokoll bezeichnet. Es gibt unterschiedliche Kommunikationsprotokolle, die sich in ihrer Funktionalität stark voneinander unterscheiden. Die wichtigsten Protokolle sind:

- TCP/IP Protokollfamilie
- OSI-Protokolle
- NetWare-Protokolle SPX/IPX
- Protokolle beim LAN-Manager

Kommunikationsprotokolle

In einem Netz können die zu übertragenen Daten verfälscht werden. Gegen die Folgen müssen entsprechende Funktionen in den Kommunikationsprotokollen enthalten sein. Im allgemeinen lassen sich diese Funktionen in drei Gruppen aufteilen:

- Fehlerkontrolle (Fault Control)
- Flußkontrolle (Flow Control)
- Überlastkontrolle (Congestion Control)

Kommunikationsprotokolle

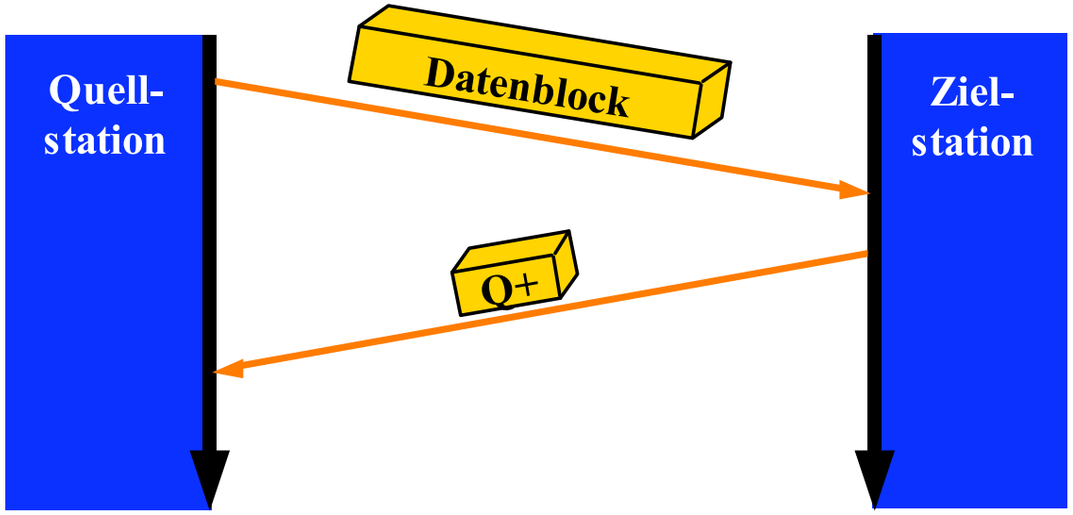
Die Fehlerkontrolle umfasst alle Maßnahmen in einem Kommunikationsprotokoll die dazu dienen, Datenverfälschungen und Datenverluste während der Übertragung zu entdecken und zu beseitigen. Die Flusskontrolle bedeutet eine gegenseitige Anpassung der Sende- und der Empfangsseite in Bezug auf die übertragene Datenmenge. Die Überlastkontrolle betrifft alle Vorkehrungen, die dazu dienen, ein Netz nicht zu überlasten.

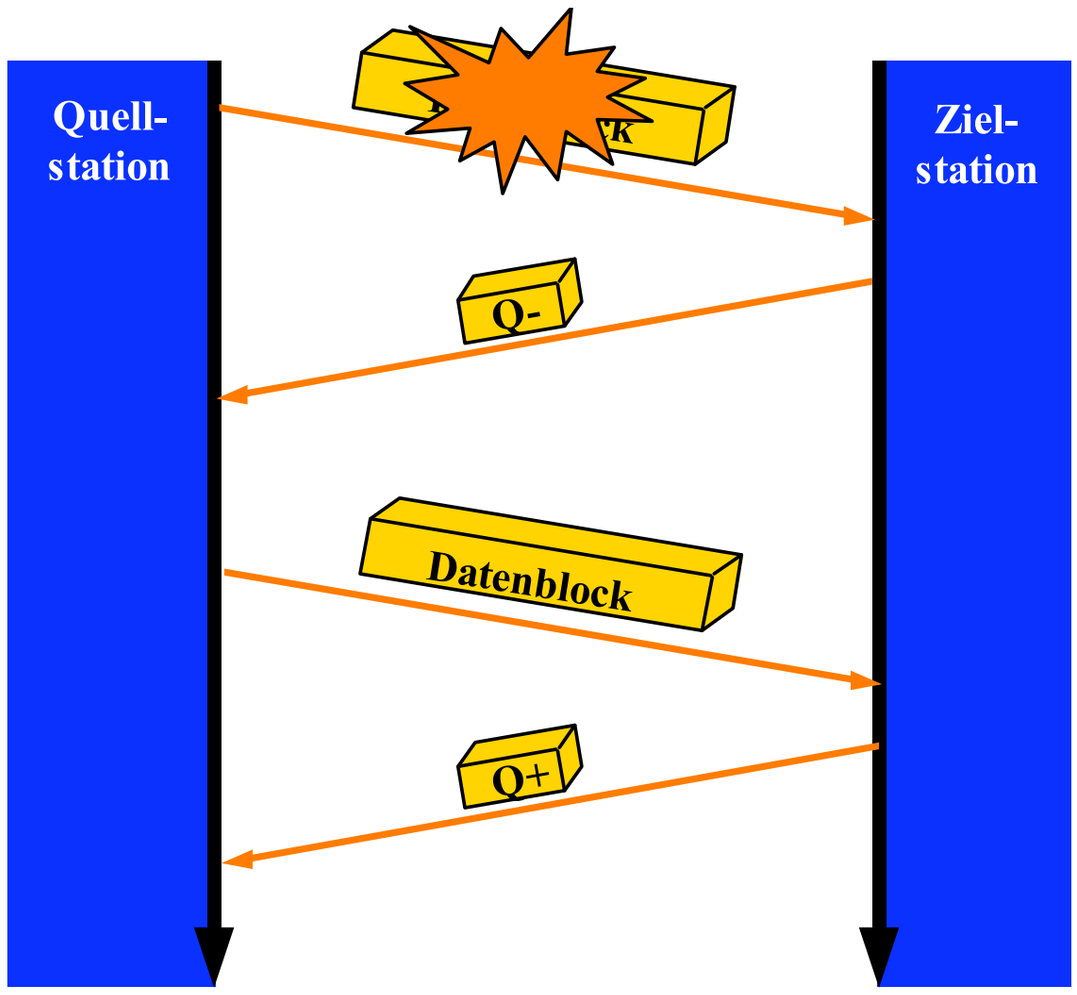
Fehlerkontrolle

Die Fehlerkontrolle hat die Aufgabe, jede fehlerhafte Situation während der Datenübertragung zu entdecken und entsprechend zu beseitigen. Sie ist Bestandteil jedes Kommunikations-protokolls und wird beim Empfänger mit Hilfe von festgelegten Quittungen (Bestätigungen) und beim Sender durch die Zeitüberwachung realisiert. Es liegen zwei „eiserne Regeln“ zugrunde:

- Datenblöcke können während der Übertragung verfälscht werden
- Datenblöcke können bei der Übertragung verloren gehen

Fehlerkontrolle

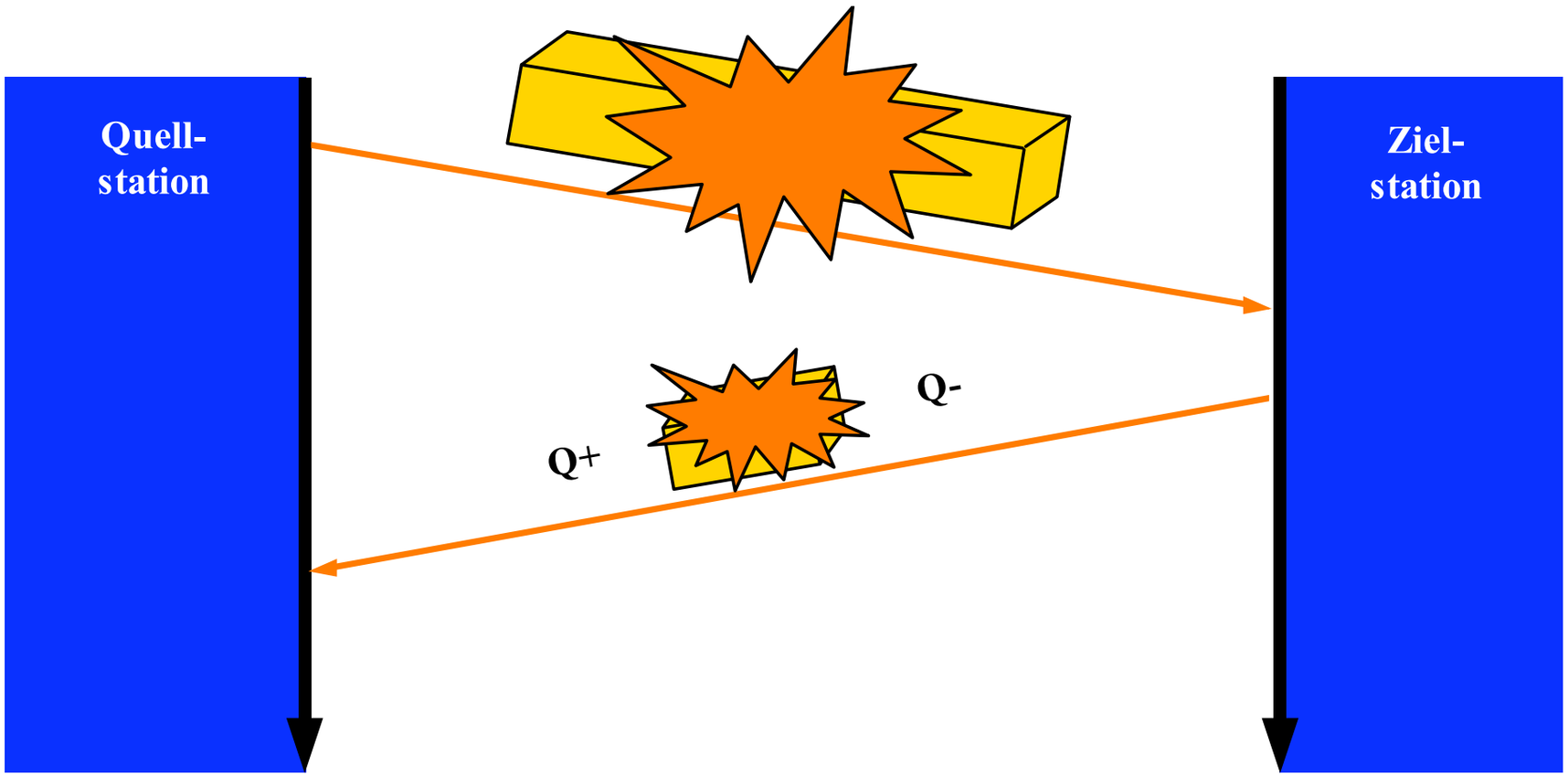




Q+: Positive Quittung

Q-: Negative Quittung

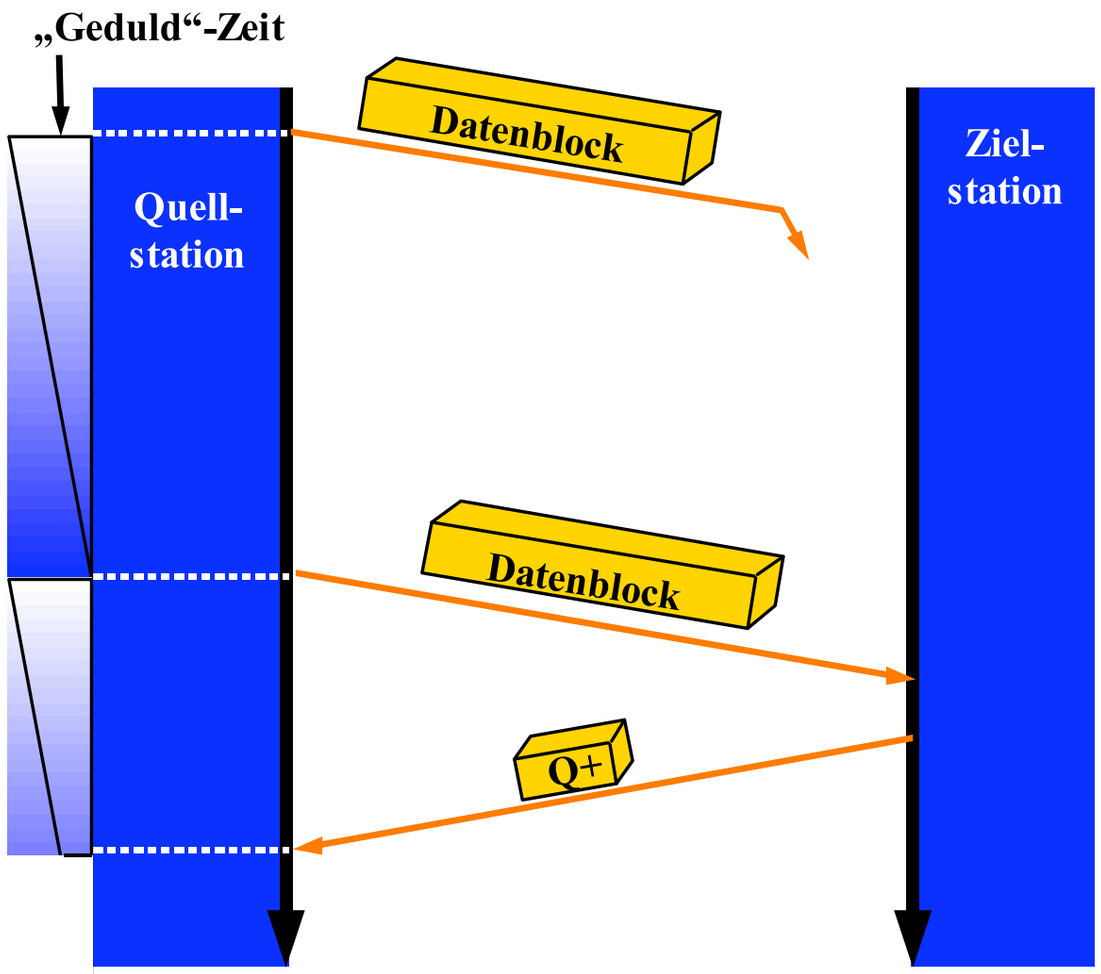
Fehlerkontrolle

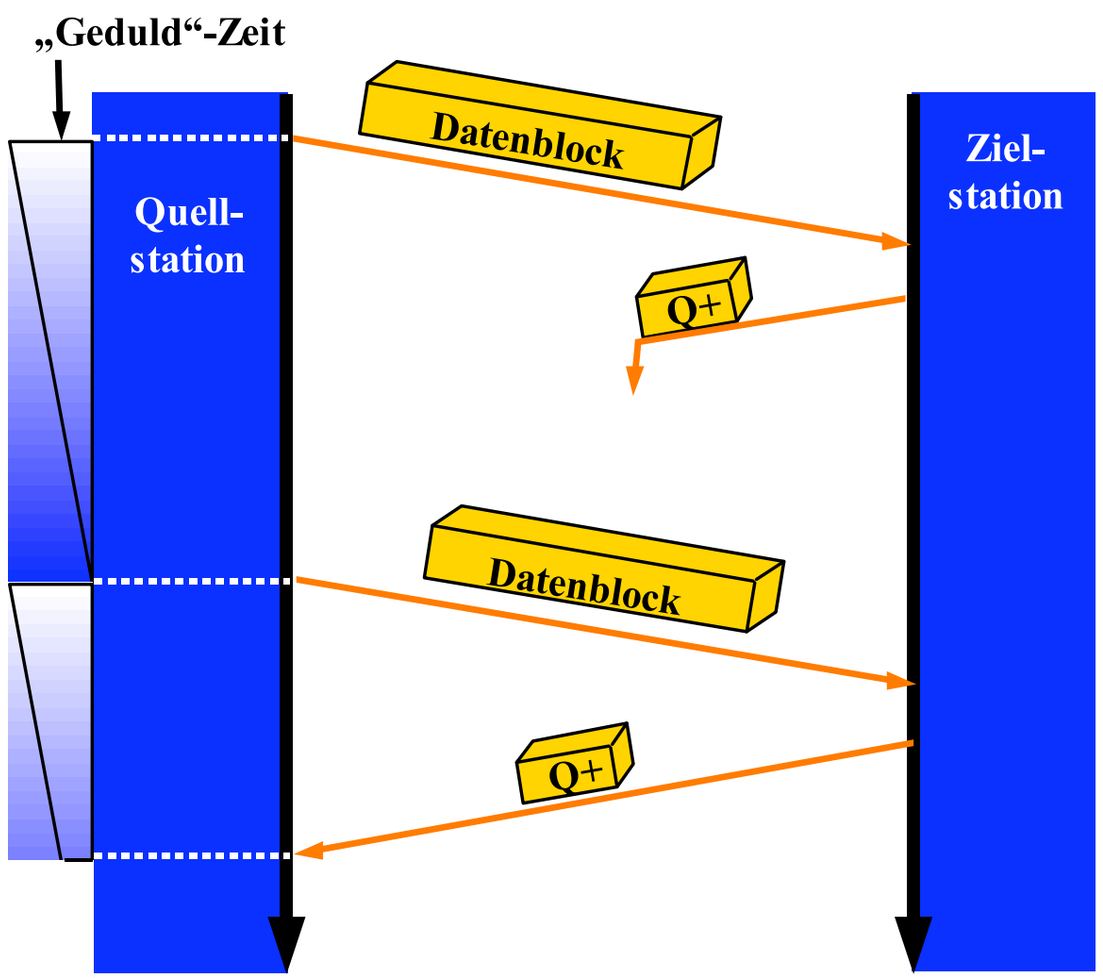


Q+: Positive Quittung

Q-: Negative Quittung

Fehlerkontrolle



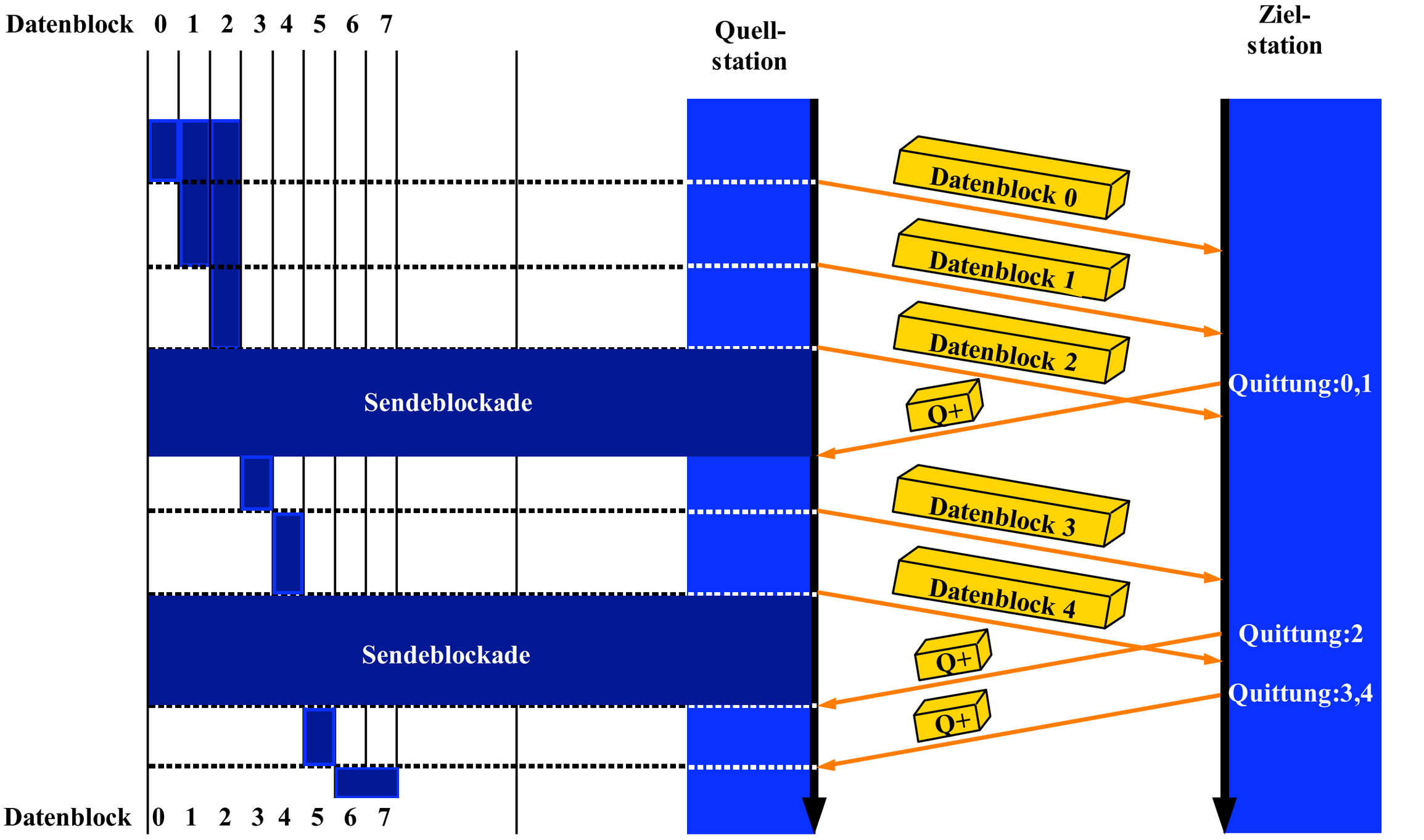


Flusskontrolle

Unter der Flusskontrolle versteht man alle Maßnahmen, die zur Anpassung der gesendeten Datenmenge der Quellstation an die Aufnahmekapazität der Zielstation führen. Die Flusskontrolle kann realisiert werden:

- mit Hilfe von Meldungen: Halt, Weitersenden,
- mit Hilfe von Krediten
- über einen Fenster-Mechanismus

Flusskontrolle



Überlastkontrolle

Ein LAN oder ein WAN hat eine bestimmte Aufnahmekapazität, d.h. zu einem bestimmten Zeitpunkt kann sich nur eine begrenzte Anzahl von Datenblöcken im Netz befinden. Wird diese Anzahl überschritten, entstehen für den Netzbenutzer folgende negative Auswirkungen:

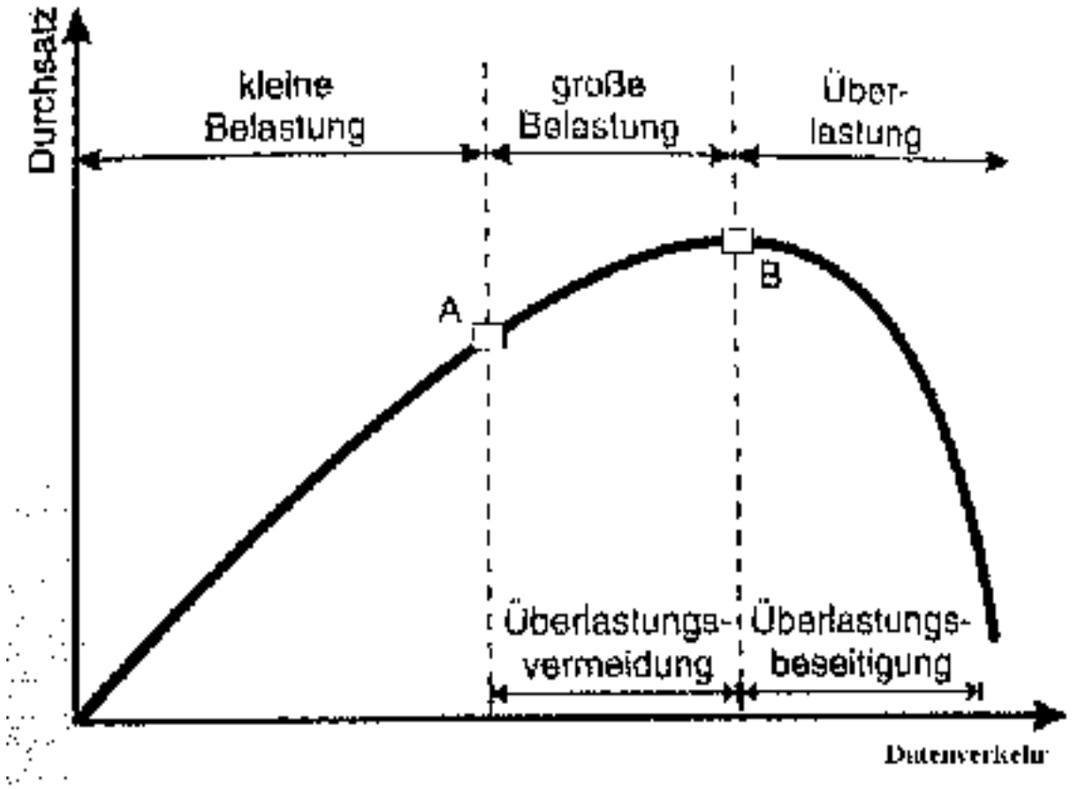
- Die Aufnahme-Puffer im Netz (in Knoten) sind voll, was dazu führt, dass die im Netz eintreffenden Datenblöcke verworfen werden müssen.
- Es bilden sich Warteschlangen von Datenblöcken vor den Übertragungsleitungen, was große Verweilzeiten der Datenblöcke im Netz verursacht. Dadurch entstehen große Verzögerungen der übertragenen Datenblöcke.

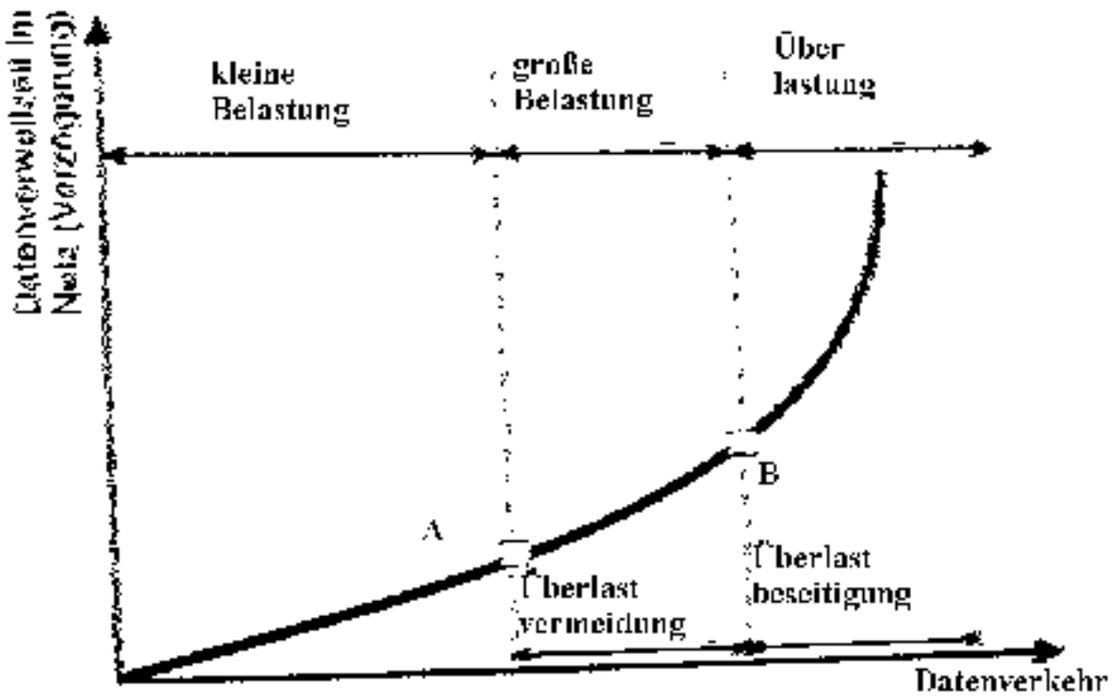
Überlastkontrolle

Bei der Überlastkontrolle (Congestion Control) werden Vorkehrungen getroffen, die verhindern, dass das Netz überlastet wird. Die wichtigsten Kriterien für die Überlastung von Netzen sind:

- Durchsatz
- Datenverweilzeit im Netz (Verzögerung)

Überlastkontrolle





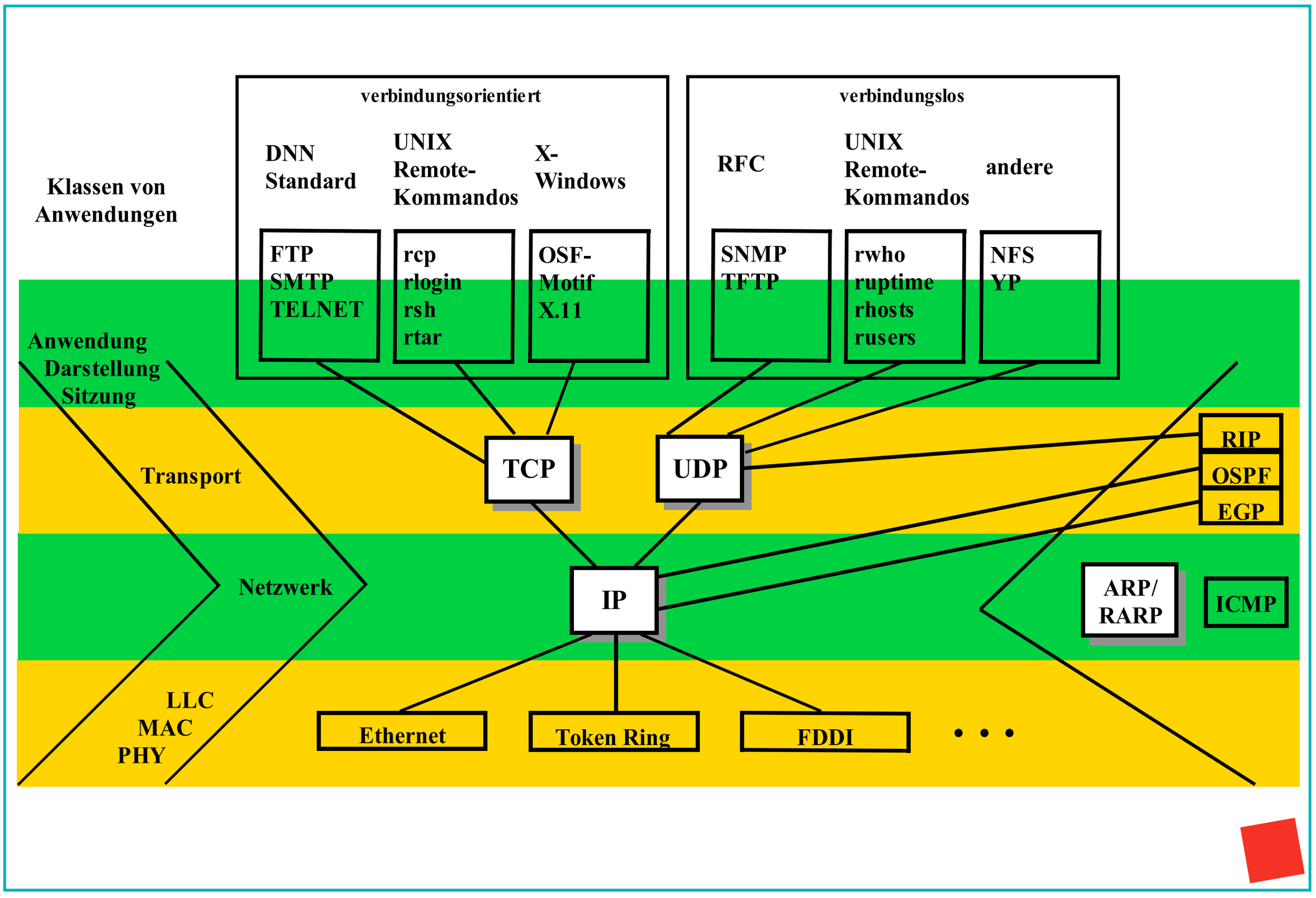
TCP/IP Protokollfamilie

Der TCP/IP Protokollsatz besteht nicht nur aus den Protokollen TCP und IP, sondern beinhaltet eine ganze Reihe weiterer Protokolle. Die verteilten Anwendungen werden in zwei Klassen aufgeteilt:

- Verbindungsorientierte Anwendungen
- Verbindungslose Anwendungen

Zu den verbindungsorientierten verteilten Anwendungen gehören diejenigen, für die eine virtuelle Verbindung zwischen zwei Endsystemen aufgebaut werden muss. Diese Anwendungen nutzen für die Kommunikation das Protokoll TCP.
Zu den verbindungslosen verteilten Anwendungen gehören diejenigen, für die keine virtuelle Verbindung zwischen zwei Endsystemen aufgebaut werden muss. Diese Anwendungen nutzen für die Kommunikation das Protokoll UDP.

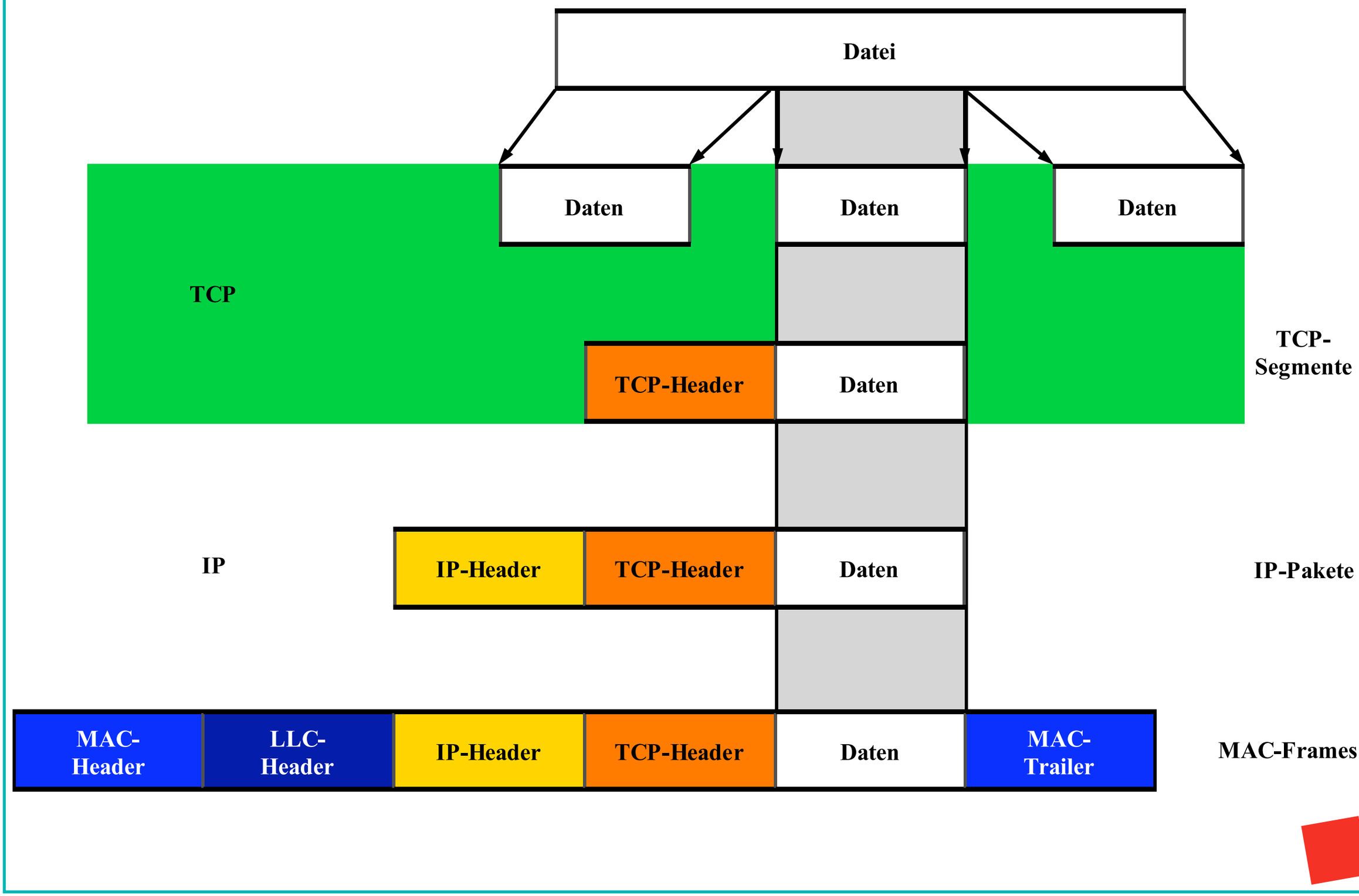
TCP/IP Protokollfamilie



TCP/IP Protokollfamilie

Bei der Datenübertragung wird die anfallende Arbeit unter den Protokollen aufgeteilt. Eine zu übertragende Datei wird in Segmente aufgeteilt. Jedes Segment wird mit einem eigenen TCP-Header versehen und bildet ein TCP-Paket. Anschließend gibt TCP das Paket an IP weiter. IP wiederum versieht das Paket mit einem IP-Header, in dem die entsprechende IP-Adresse aufgeführt ist. Schließlich wird das IP-Paket an ein Netzwerk weitergeleitet. Dort kommt ein MAC-Header und der übliche MAC-Trailer hinzu. Jetzt erst wird das Datensegment in Form eines MAC-Frames über das Netz zum Ziel geschickt werden. Am Ziel angekommen, erfolgt die Umwandlung des Frames in umgekehrter Reihenfolge.

Übertragung nach TCP/IP



IP Protokoll

Das IP-Protokoll ist verbindungslos und unzuverlässig. Das IP-Protokoll gibt keine Garantie für die Zustellung der Pakete an den Zielrechner. Die einzelnen Pakete werden voneinander unabhängig zum Ziel abgeschickt. Für die Einordnung der empfangenen IP-Pakete in ihre korrekte Reihenfolge und deren Zusammensetzung zu einer Datei (Nachricht) ist das Protokoll TCP verantwortlich. Die wichtigsten Angaben, die den zu übertragenen Daten vom IP-Protokoll hinzugefügt werden, sind die IP-Adressen vom Quell- und vom Zielrechner. Dadurch ist das eigenständige Versenden der einzelnen IP-Pakete möglich.

IP Header

Version	Header Length	TOS	Total Length	
Identification			Flags: 0 DF MF	Fragement Offset
Time to live		Protocol	Checksum	
Source-IP-Address				
Destination-IP-Address				
Option				Padding
TCP-Header				
Nutzdaten				

IP Header Protokoll Nummern

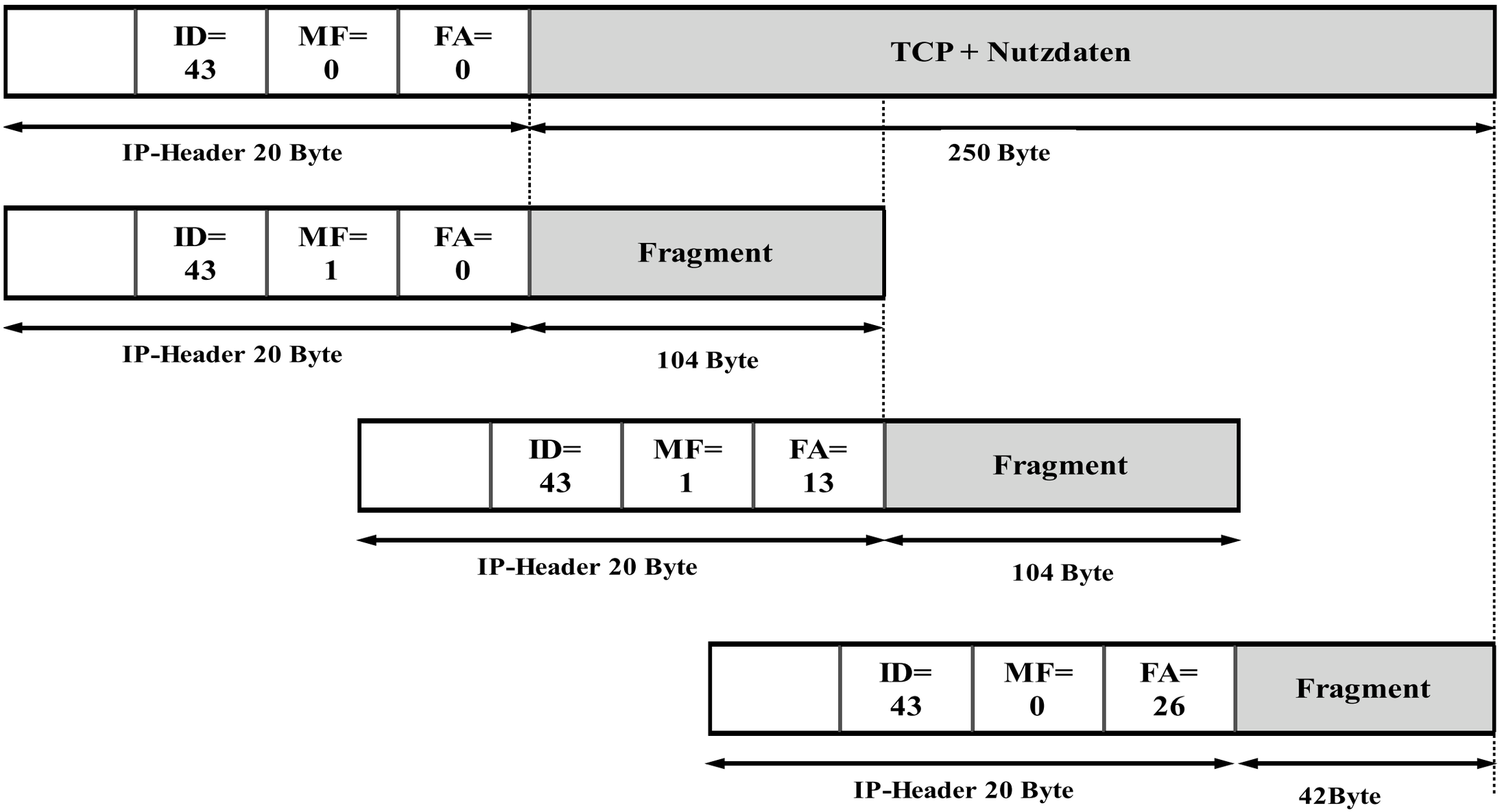
Nummer	Abkürzung	Bezeichnung
1	ÎCMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
6	TCP	Transmisssion Control
8	EGP	Exterior Gateway Protokol
17	UDP	User Datagramm
20	HMP	Host Monitoring
22	XNS-IDP	XEROX NS IDP

Nummer	Abkürzung	Bezeichnung
27	RDP	Reliable Data Procol
28	IRTP	Internet Reliable Transaction
29	ISO-TP4	ISO Transport Protocol Class 4
30	NETBLT	Bulk Data Transfer Protocol
80	ISO-IP	ISO Internet Protocol
86	DGP	Dissimilar Gateway Protocol
87	TCF	Transparent Computing Facility
89	OSPF	Open Shortest Path First

IP Paket Fragmentierung

Abhängig vom Übertragungsmedium wird die maximale Größe des IP-Pakets in Form der Maximum-Transfer-Unit (MTU) festgelegt. Zur Anpassung an unterschiedliche Medien, ist IP in der Lage, die Pakete entsprechend den Anforderungen zu fragmentieren. In einem X.25-Netz dürfen Pakete nicht größer als 128 Bytes sein, während das Ethernet eine Frame-Lenge von 1526 Bytes erlaubt. Unter Fragmentierung versteht man die Fähigkeit des IP-Protokolls, in einem Netzknoten oder dem Quellrechner die zu sendenden IP-Pakete aufzuteilen, so dass sie zum nächsten Netzknoten oder Zielrechner übertragen werden können.

IP Paket Fragmentierung



IP Paket Fragmentierung

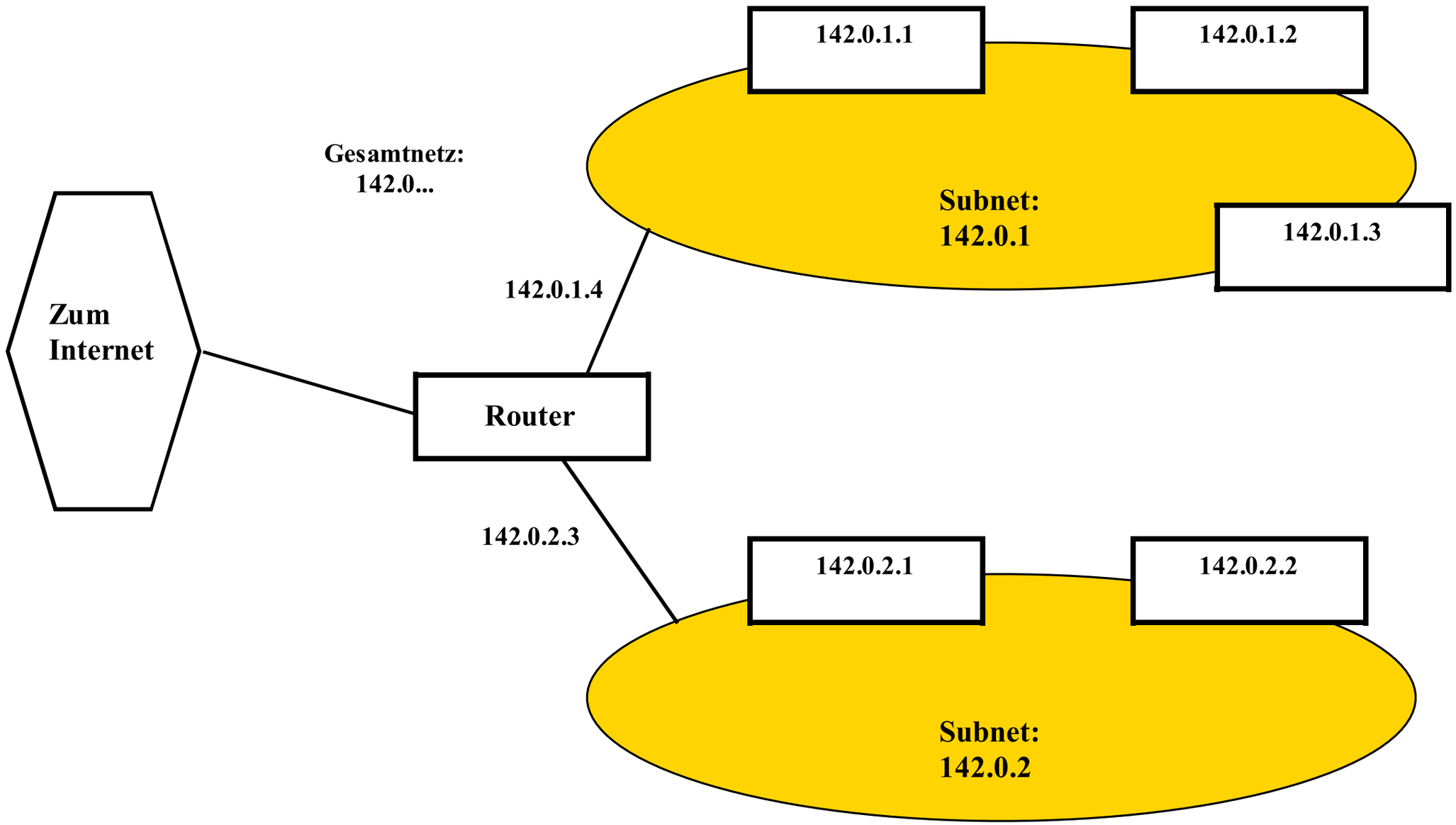
Die Größe des IP-Pakets liegt bei maximal 65536 Bytes. Wenn man die minimale Länge von 20 Bytes des IP-Headers berücksichtigt, bleiben für die weiteren Daten und den TCP-Header noch 65516 Bytes. Viele Netz-Implemtationen haben eine MTU von 576 Bytes die von jeder TCP/IP Implementation unterstützt werden muss. Bei Ethernet ist die MTU 1500 Bytes. Beim FDDI z.B. 4500 Bytes.

Internet Adressen

Das IP-Protokoll übernimmt die Adressierung und das Routing in einem Netz bzw. in einem Netzwerk-Verbund. Für die Adressierung wird eine 32 Bit lange Internet-Adresse benutzt (Bei IPV6 128 Bit). Diese Adressen werden in vier Oktetts beschrieben, die wiederum dezimal dargestellt werden, z.B. 141.64.128.243. Eine Internet-Adresse hat folgende Struktur: Netz-ID, Host-ID (Stations-ID).

Bei der Vergabe in IP-Adressen muss man darauf achten, dass die Adressen aller in einem physikalischen Netz liegenden Stationen (Nodes) sich nur in dem Node-Teil unterscheiden und dass keine IP-Adresse doppelt vorkommt.

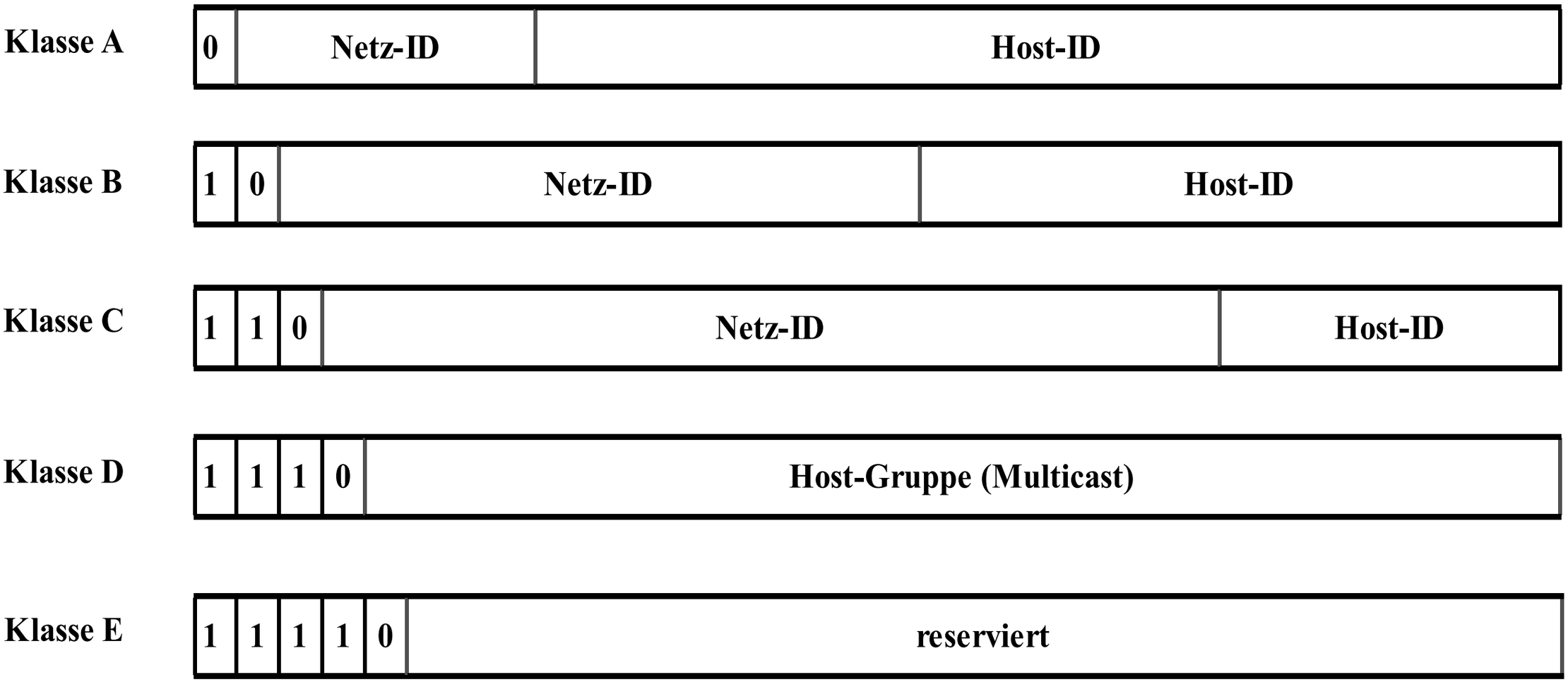
Internet Adressen



Internet Adressen

Bei der Adressvergabe unterscheidet man fünf Klassen von IP-Adressen. Je nach Anzahl der im Netz vorgesehenen TCP/IP-Hosts bekommt man eine Adresse einer entsprechenden Klasse zugeteilt. Über die Netzadressen wird, unter anderem, eine Unterteilung in verschiedene Anwendungen (Wissenschaft, Militär) und in Installationsorte (USA, Europa,...) vorgenommen.

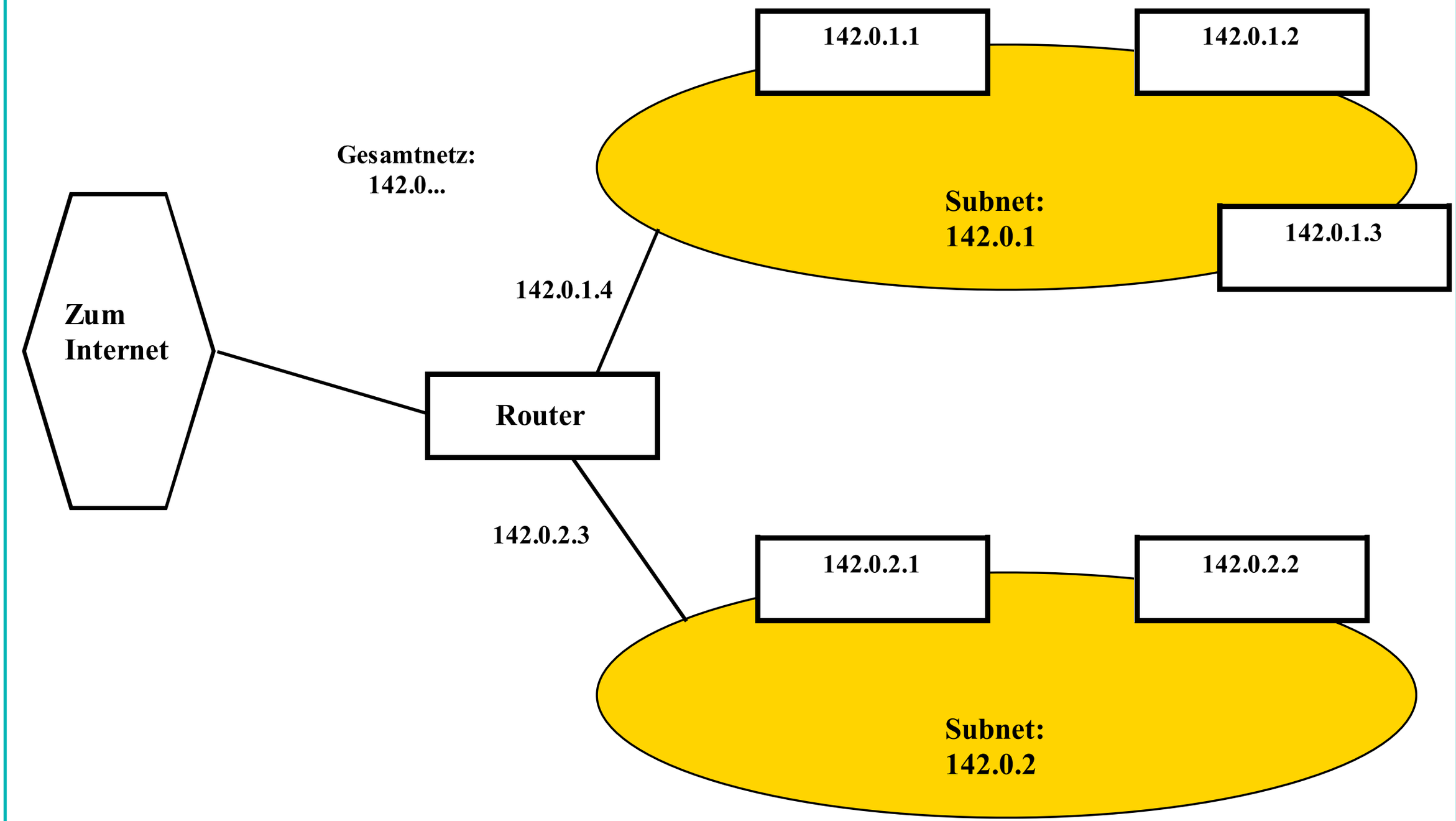
Internet Adressen



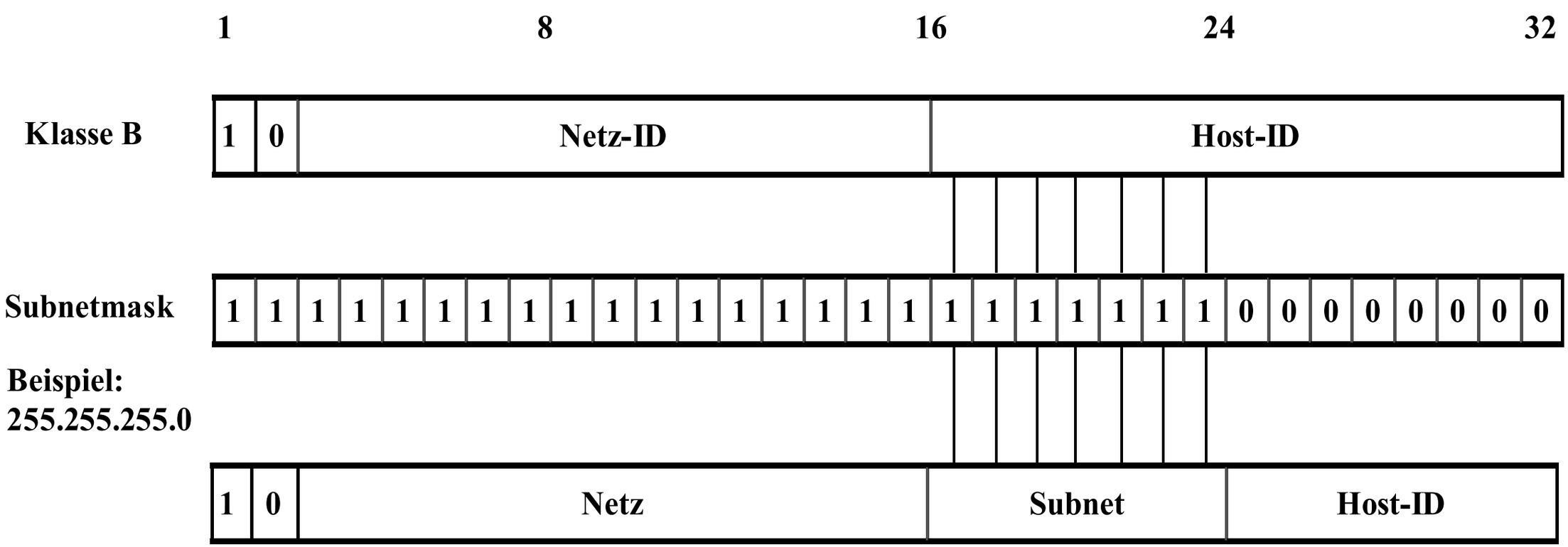
Subnetze

Subnetze entstehen wenn autonome Netze in mehrere physikalische oder logische Netze aufgeteilt werden. Subnetze sind somit zwei oder mehrere physikalische Netze, die eine gemeinsame Netzidentifikation besitzen. Um eine Routing-Möglichkeit auf großen Campus-Netzen zu realisieren, legt man Subnetze auf IP-Ebene fest. Für die Bildung von Subnetzen definiert man eine Maske, die den Anteil von Hostbits von den Netzbits separiert.

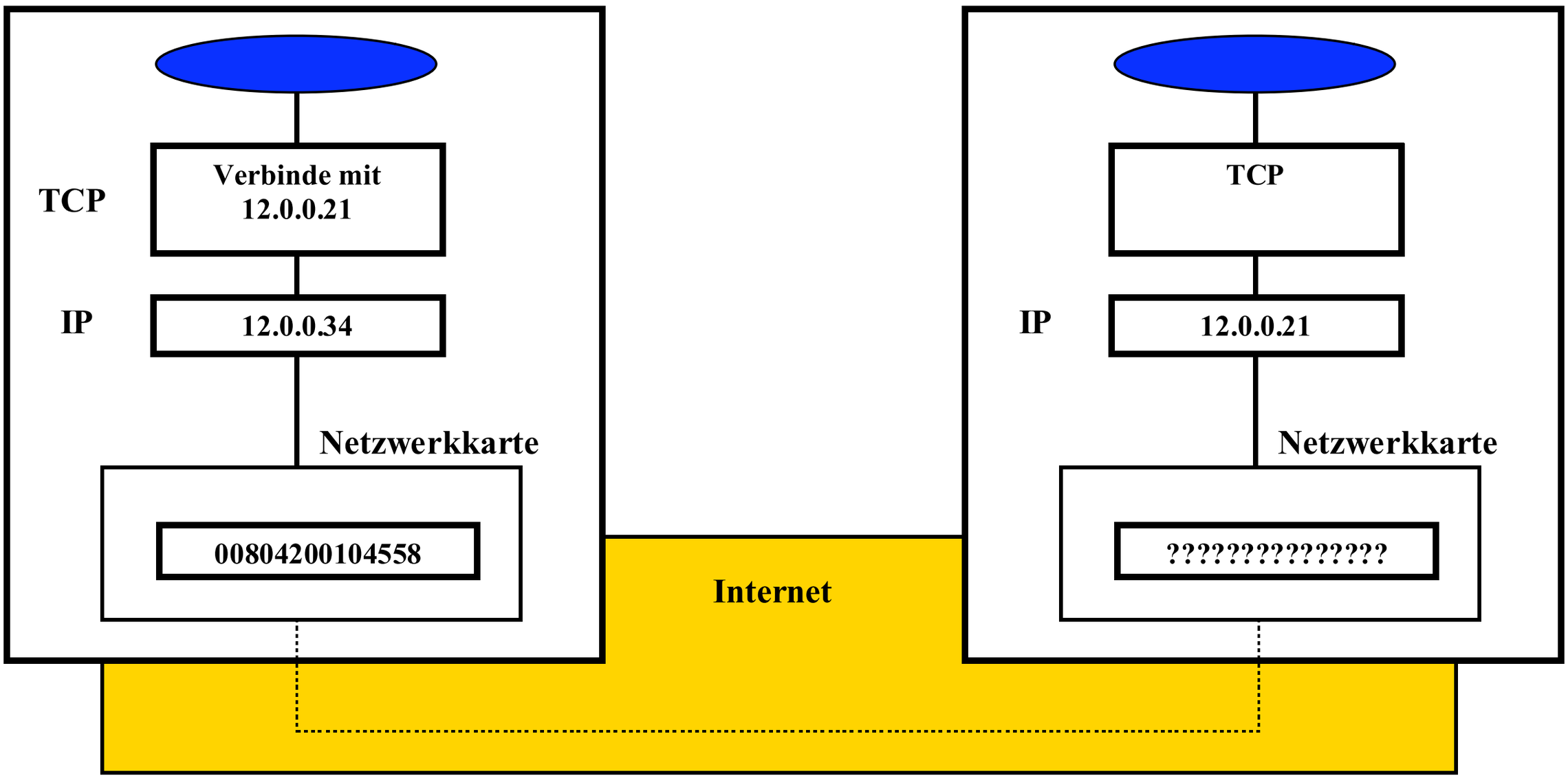
Subnetze


Gesamtnetz:
142.0...
Zum
Internet
Router
142.0.1.4
142.0.2.3
142.0.1.1
142.0.1.2
142.0.1.3
Subnet:
142.0.1
142.0.2.1
142.0.2.2
Subnet:
142.0.2

Subnetze


1
8
16
24
32
Klasse B
1
0
Netz-ID
Host-ID
Subnetmask
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0
Beispiel:
255.255.255.0
1
0
Netz
Subnet
Host-ID

ARP/RARP


TCP
Verbinde mit
12.0.0.21
IP
12.0.0.34
Netzwerkkarte
00804200104558
Internet
TCP
IP
12.0.0.21
Netzwerkkarte
??????????????

ARP/RARP

In einem Netzwerk existiert immer das Problem, dass eine bestimmte Zuordnung von einer logischen Schicht –3- Adresse (IP-Adresse) zu einer physikalischen Schicht –2- Adresse (MAC-Adresse) getroffen werden muss. Früher wurde das Problem als statische Tabellen in jedem Rechner gelöst, in die man manuell alle Zuordnungen zwischen MAC- und IP-Adressen eintragen musste. Heutzutage werden diese Zuordnungen dynamisch mit dem Protokoll ARP (Address Resolution Protocol) realisiert.

ARP/RARP

Netzwerk Typ		Protokoll Typ
HLEN	PLEN	Betriebs Code
Sender MAC		
Sender MAC		Sender PA
Sender PA		Target MAC
Target-MAC		
Target-PA		

Netzwerk Typ:	1=Ethernet; 6=IEEE 802.2
Protokoll Typ:	2048= IP
HLEN:	2=16 Bit MAC; 6=48 Bit MAC;
PLEN:	4=32 Bit IP Adresse
Betriebs Code:	1=Request; 2=Reply
Sender MAC Sender-PA	Hardwareadresse IP-Adresse des Senders
Target MAC Target-PA	Hardwareadresse IP-Adress des Empfängers

ARP/RARP

Das Protokoll RARP (Reverse Address Resolution Protocol) ist für Stationen gedacht, die Ihre IP-Adresse nicht slbst speichern können. RARP ist das gegenstück zu ARP, d.h. RARP bietet Funktonen, die es ermöglichen, aus einer bekannten MAC-Adresse die zugehörige IP-Adresse zu finden. Beim RARP ist es notwendig, einen speziellen Server festzulegen in dem eine RARP Tabelle aufgebaut wird. Dieser Server sucht in seiner Tabelle nach der IP-Adresse, die mit der MAC-Adresse im Anforderungspaket übereinstimmt, und gibt die gesuchte IP-Adresse als RARP-Antwort bekannt.

SLIP/PPP

Es wurden spezielle Versionen des IP-Protokolls entwickelt um die Kommunikation zwischen den TCP/IP-Anwendungen über Punkt-zu-Punkt Anwendungen zu ermöglichen. Es handelt sich dabei um:

- SLIP (Serial Line Internet Protocol)
- PPP (Point-to-Point Protocol)

SLIP/PPP

SLIP wurde in RFC 1055 festgelegt und ist ein einfaches Protokoll für die Verbindung von TCP/IP Anwendungen über eine serielle Leitung (z.B. Standleitung oder ISDN-B-Kanal-Verbindung). Das SLIP stellt ein zeichenorientiertes Protokoll der Sicherungsschicht dar. Für die Übertragung eines IP-Pakets über eine Punkt-zu-Punkt-Verbindung sind nicht alle Angaben im IP-Header notwendig. Es gibt ein Verfahren für die Komprimierung von IP-Angaben bei dieser Übertragungsart. Dieses Verfahren ist in RFC 1144 festgelegt und ist unter dem Namen „Van-Jacobsen-Verfahren“ bekannt. Nach diesem Verfahren wird der gesamte TCP- und IP-Overhead mit insgesamt 40 Bytes auf bis zu 3 bis 5 Bytes reduziert. Das Protokoll SLIP mit Komprimierung wird als CSLIP (Compressed SLIP) bezeichnet.

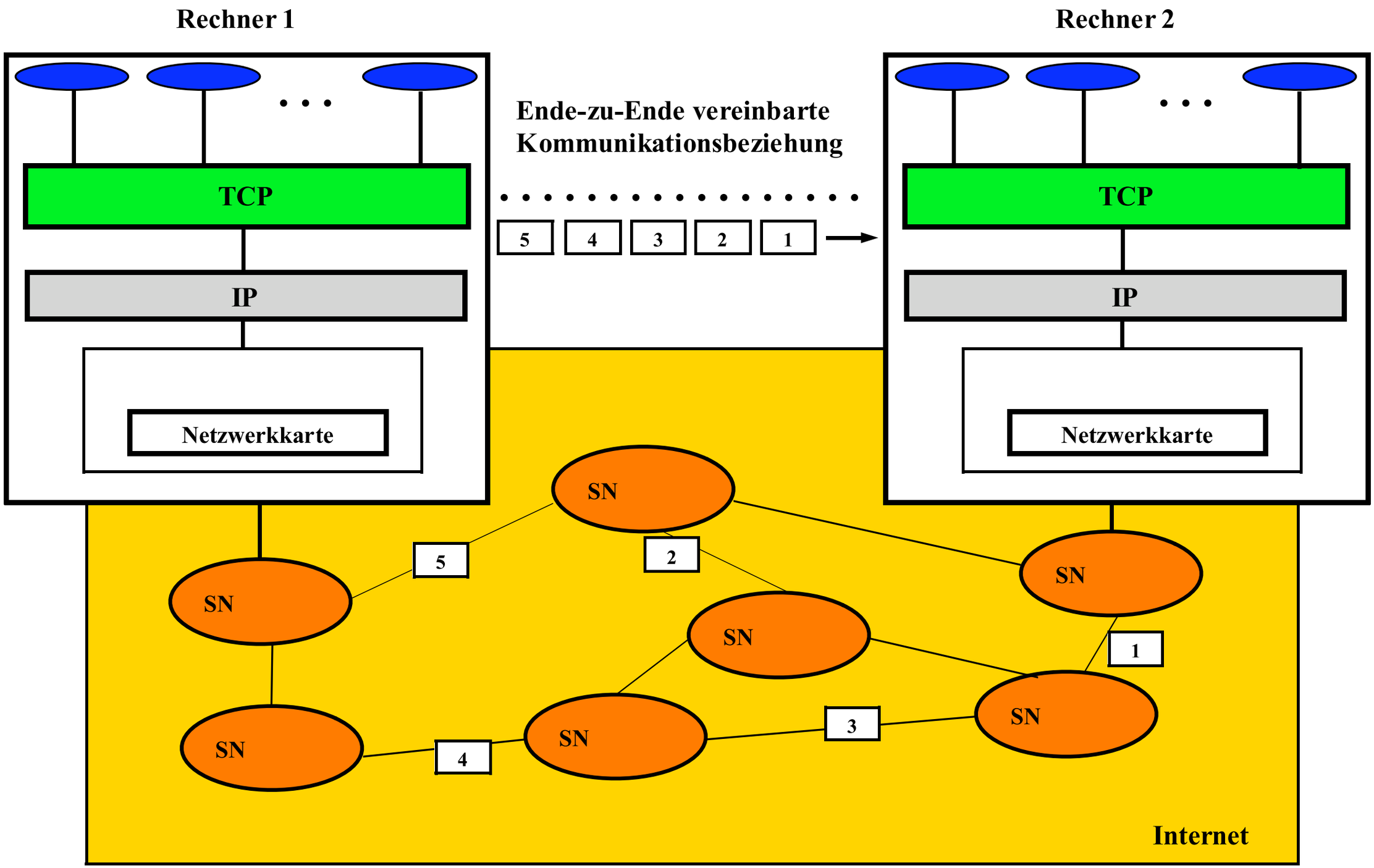
SLIP/PPP

Das Protokoll PPP (RFCs 1548, 1332) hat die gleiche Funktionalität wie SLIP, entspricht aber dem bitorientierten Protokoll HDLC. Das PPP hat die gleichen Vorteile gegenüber dem SLIP wie das Protokoll HDLC gegenüber den zeichenorientierten Sicherungsprotokollen.

Zusammenspiel TCP und IP

Die beim IP-Protokoll benutzte IP-Adresse reicht nicht aus, um eine verbindungsorientierte Ende-zu-Ende Verbindung aufzubauen. Bevor zwei Programme miteinander kommunizieren können, müssen sich Kommunikationsendpunkte miteinander verständigen. Diese Punkte werden als „Empfänger-Port“ und „Sender Port“ bezeichnet und müssen als Adresse bei den Protokollangaben in den verschiedenen Schichten verwendet werden. Somit müssen beide Seiten vorher eine Portnummer vereinbart haben, unter der der passive Partner auf das Zustandekommen einer Verbindung wartet.

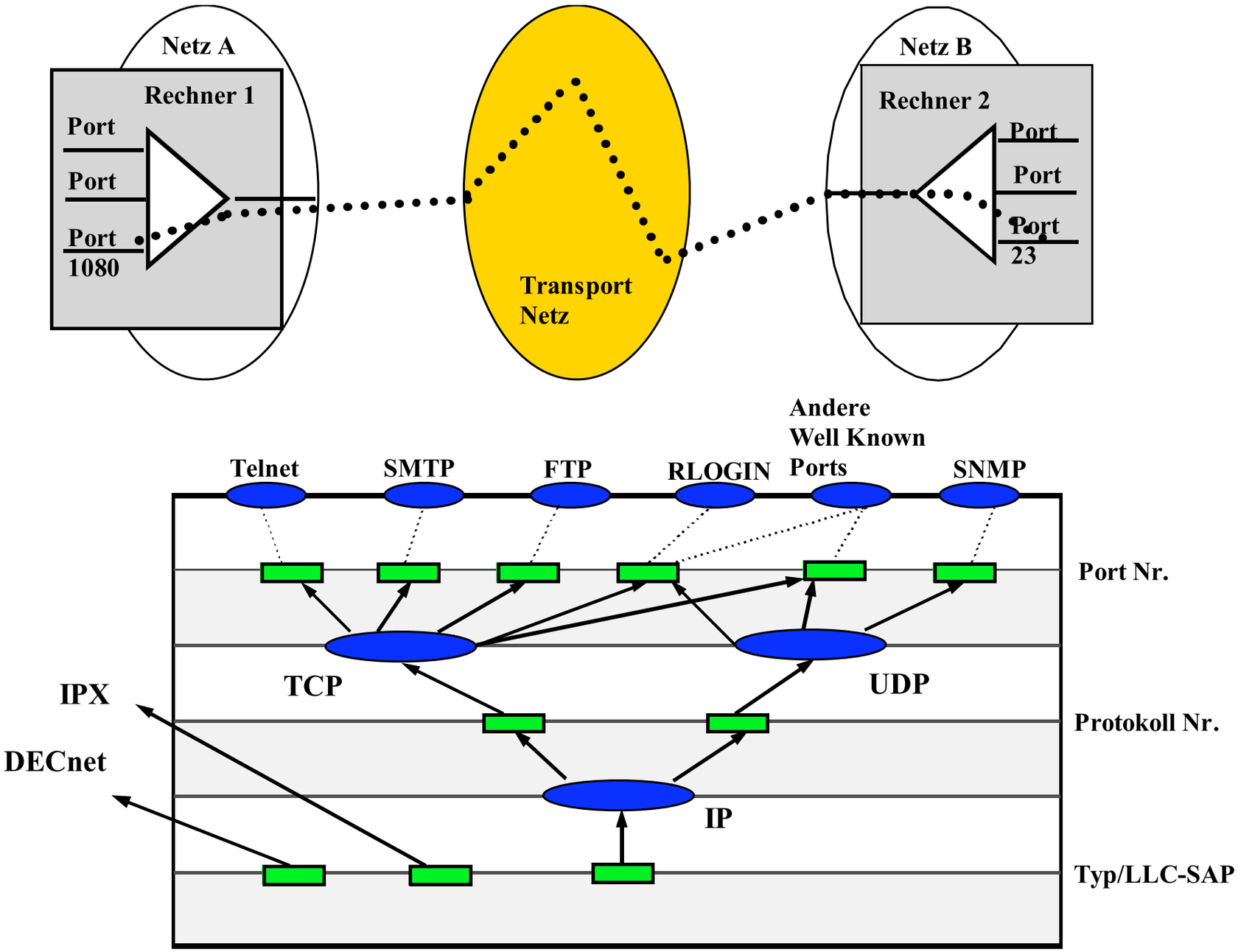
Zusammenspiel TCP und IP



Zusammenspiel TCP u. IP

Es ist möglich, dass zu einem bestimmten Zeitpunkt mehr als eine Anwendung die Protokolle TCP/IP und UDP/IP benutzen kann. Um das zu realisieren, muss IP mit TCP bzw. UDP entsprechend zusammenarbeiten. Die beiden Tuple IP-Adresse und Port-Nummer des Senders und Empfängers definieren einen gemeinsamen Kommunikationsendpunkt, auch Socket genannt. Jedem Socket steht im Rechner ein reservierter Speicherplatz als Kommunikationspuffer zur Verfügung. Die zu übertragenden und empfangenden Daten werden jeweils in dem für die Sockets reservierten Kommunikationspuffer abgelegt.

Zusammenspiel TCP und IP

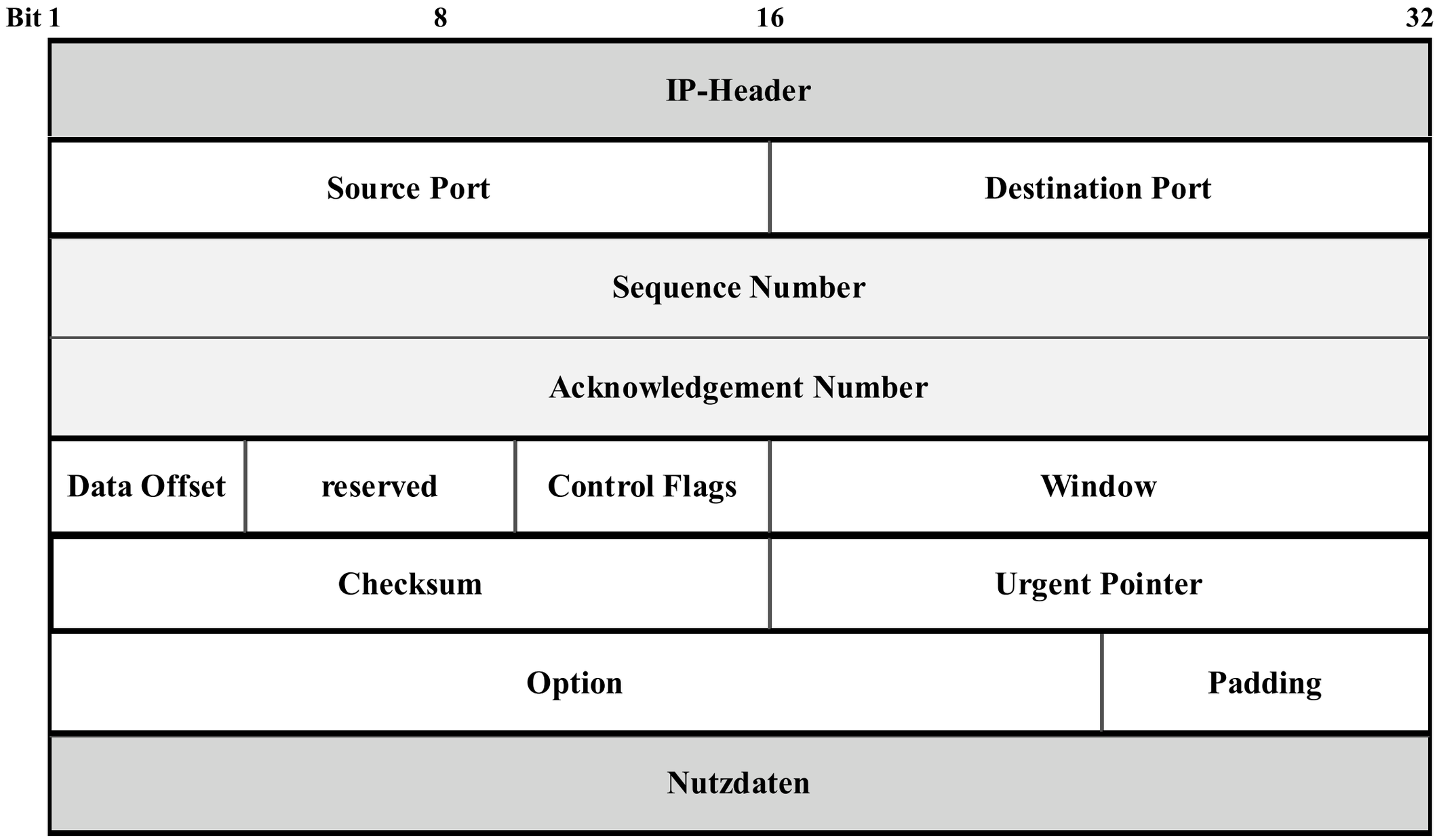


TCP-Protokoll

Beim TCP-Protokoll wird eine virtuelle und duplex-fähige Ende-zu-Ende-Verbindung zwischen einem Quell- und einem Zielrechner aufgebaut. Über diese Verbindung werden die Daten in Form von festgelegten Datenblöcken (TCP-Pakete) ausgetauscht. Damit ist TCP ein verbindungsorientiertes Ende-zu-Ende Protokoll mit folgenden weiteren Besonderheiten:

- Abstimmung der Länge von TCP-Paketen
- Segmentierung der zu sendenden Dateien (im Quellrechner)
- Sicherung der Reihenfolge der TCP-Pakete durch Sequenznummern
- Wiederherstellung von Dateien durch die Zusammensetzung von empfangenen TCP-Paketen (im Zielrechner)
- Aufforderung des Quellrechners zur wiederholten Übertragung von gestörten oder verloren gegangenen TCP-Paketen

TCP Header


Bit 1
8
16
32
IP-Header
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Data Offset
reserved
Control Flags
Window
Checksum
Urgent Pointer
Option
Padding
Nutzdaten

TCP-Protokoll

TCP verhindert den gleichzeitigen Verbindungsaufbau zwischen zwei Stationen, d.h. nur eine Station kann den Aufbau initiieren. Des weiteren ist es nicht möglich, einen mehrfachen Aufbau einer Verbindung durch den Sender aufgrund eines Timeouts des ersten Verbindungsaufbau-wunsches zu generieren.

Der Datenaustausch erfolgt nach dem Verbindungsaufbau. Gehen Daten verloren, dann wird nach Ablauf eines Timeouts die Wiederholung der fehlerhaften Segmente gestartet. Durch die Sequenznummer ist es möglich 2^32 –1 Daten pro bestehender Verbindung zu übertragen.

TCP-Protokoll

Die Flusskontrolle nach dem Fenster-Mechanismus (Window-Feld) erlaubt es dem Empfänger, dem Sender mitzuteilen, wie viel Pufferplatz er zum Empfang der Daten zur Verfügung stehen hat. Ist der Empfänger zu einem bestimmten Zeitpunkt der Übertragung einer höheren Belastung ausgesetzt, kann er dies dem Sender über das Window-Feld bekannt geben.

Jedes übertragene Paket unterliegt einer Zeitüberwachung (Retransmission Time); das bedeutet, dass ein Empfänger nach einer bestimmten Zeitdauer eine Quittung über die erhaltenen Pakete aussenden muss. Da diese Zeitdauer sehr stark von der aktuellen Belastung des Netzes abhängt, muss der Retransmission Timer für jedes Paket neu berechnet und eingestellt werden.

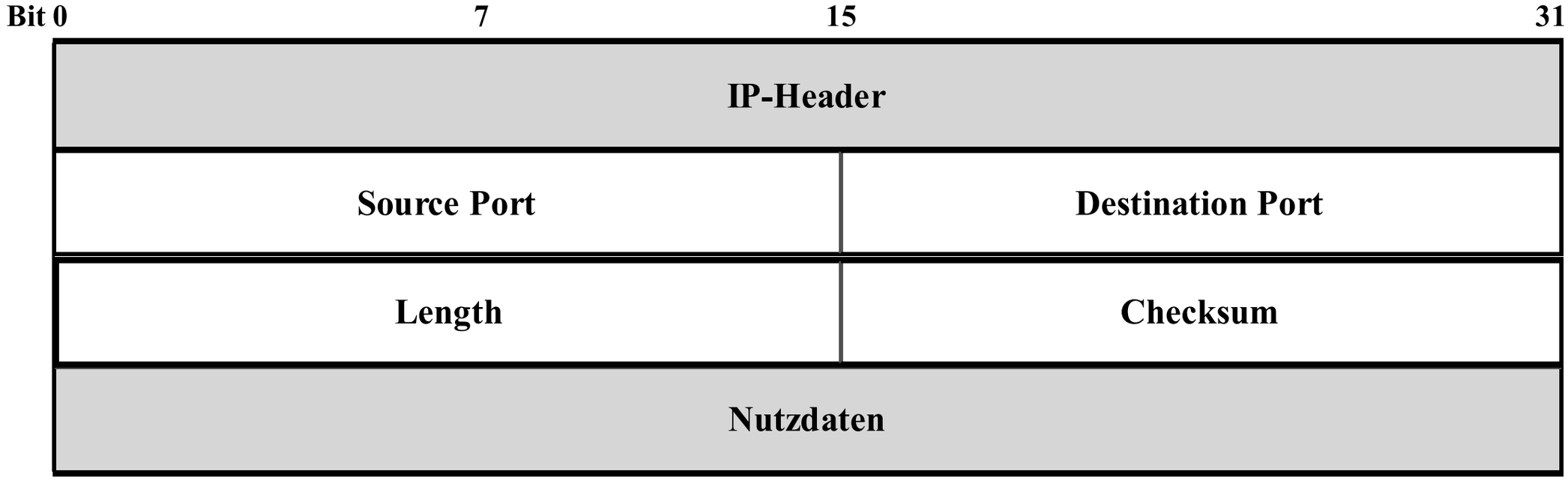
UDP-Protokoll

Bei UDP (User Datagram Protocol) handelt es sich um den einfachsten verbindungslosen Dienst, der auf IP aufsetzt. Durch UDP können Anwendungen Datagramme senden und empfangen. UDP bietet keine gesicherte Übertragung und keine Flusskontrolle.

Das UDP wird für das Network File System (NFS) sowie für das Versenden von Broadcast-Nachrichten oder innerhalb eines Netzwerk-Managements (z.B. SNMP) genutzt.

Aufgrund des Einsatzbereiches von UDP ist der Header entsprechend klein.

UDP Header


Bit 0
7
15
31
IP-Header
Source Port
Destination Port
Length
Checksum
Nutzdaten